

Dr. Raymond J. Juzaitis
Associate Director for Nonproliferation, Arms Control, and International Security
Lawrence Livermore National Laboratory
University of California

September 22, 2005

Hearing of the Committee on Homeland Security
Subcommittee on Prevention of a Nuclear and Biological Attack
U.S. House of Representatives

COUNTERING THE THREAT OF NUCLEAR TERRORISM

Hearing of the Committee on Homeland Security
Subcommittee on Prevention of a Nuclear and Biological Attack
U.S. House of Representatives

September 22, 2005

Raymond J. Juzaitis
Lawrence Livermore National Laboratory
University of California

OPENING REMARKS

Mr. Chairman and members of the committee, thank you for the opportunity to appear before you today. I am the Associate Director for Nonproliferation, Arms Control, and International Security at the Lawrence Livermore National Laboratory (LLNL), which is administered by the University of California for the Department of Energy's National Nuclear Security Administration (NNSA).

LLNL is a national security laboratory, established in 1952 to strengthen U.S. nuclear deterrence. As a principal participant in the Stockpile Stewardship Program, we help maintain confidence in the U.S. deterrent and its nuclear weapons stockpile in the absence of nuclear testing. We are also key contributors to critical national programs aimed at reducing the threat posed by the proliferation and potential terrorist acquisition of nuclear weapons and other weapons of mass destruction (WMD).

At LLNL, we take an integrated, systems approach to the interrelated challenges of nonproliferation, counterproliferation, counterterrorism, and homeland security. We address all of the phases of the WMD threat (indications and warning, prevention and detection, response and recovery), the different types of threat (nuclear, radiological, chemical, biological, high explosive, cyber), and the various threat "players" (declared and de-facto weapons states, overt and covert proliferators, state-sponsored and transnational terrorist groups). We integrate science, technology, and analysis as we assess the capabilities, motivations, and intentions of proliferators and terrorists, devise technologies and systems to detect proliferation-related activities and smuggled WMD materials, and collaborate with policy makers, the intelligence and defense communities, emergency planners, and first responders in developing capabilities for dealing with WMD proliferation or terrorism. We partner with industry, academia, and other research institutions to bring the full weight of the U.S. scientific community to bear on these most pressing national security challenges. In addition, we work closely with customers and end-users to ensure that the technological solutions we develop meet their real-world operational needs.

Well before September 11, 2001, LLNL was addressing the threat of WMD terrorism. In 1996, LLNL was requested by the Director of Central Intelligence and the Deputy Secretary of Energy to organize a study of the threat posed by terrorist groups using WMD against the U.S. The so-

called Livermore Study Group (comprised of 20 experts from the Intelligence Community, DOD, DOE, FBI, State Department, Congress, U.S. industry, and academia) developed nuclear, chemical, and biological threat scenarios to identify key needs. They constructed an end-to-end framework for dealing with the WMD terrorism threat and made specific recommendations with respect to government structure, policy and legal changes, and science and technology to address the most critical gaps thus identified. One of the group's key recommendations was for a national program integrated across the entire federal system to comprehensively address the threat of WMD terrorism.

“DEFENSE IN DEPTH” TO COUNTER NUCLEAR TERRORISM

Nuclear terrorism is an enduring threat. The principles of nuclear weapons cannot be un-invented, and the hundreds of tons of weapons-usable nuclear material generated since the 1940s cannot be un-produced. The future stability of some of today's nuclear weapon states is not assured, more countries may join the “nuclear club,” and non-state adversaries and extremist groups beyond Al Qaeda may arise.

Countering the terrorist nuclear threat requires a “defense in depth”—namely, an integrated system of systems comprised of multiple programs and activities aimed at anticipating, detecting, and interdicting the threat as close to the source and as far from the target as possible. Many of the elements of such a defense in depth are already in place.

The first lines of defense—securing nuclear weapons and weapons-usable materials at their source—are embodied by the Cooperative Threat Reduction (DOD) and the Material Protection, Control, and Accounting (DOE) programs, which were established in the 1990s after the collapse of the Soviet Union. Additional layers of defense are provided by the Second Line of Defense (DOE) and Megaports (DOE) programs as well as the newly established Proliferation Security Initiative (DOD), which are enhancing capabilities for detecting and interdicting nuclear materials at foreign border crossings, airports, seaports, and while in transit.

At the other end of the defense spectrum are long-standing national nuclear incident response programs. These include the Nuclear Assessment Program (originally DOE, transferred to DHS in 2003) for evaluating communicated nuclear threats and nuclear smuggling cases, the Radiological Assistance Program (DOE) for assisting local response entities, the Accident Response Group (DOE) for handling accidents involving U.S. nuclear weapons, the Joint Technical Operations Team (DOE) for locating and dealing with a terrorist nuclear device, Triage (DOE) and Reachback (DHS) programs for providing expert technical assistance to responders in the field, the Consequence Management program (DOE) for dealing with the immediate aftermath of a nuclear incident, and the Nuclear Attribution program (DOD, DOE, DOJ, DHS) for identifying the origins of terrorist nuclear material or a nuclear device,

LLNL provides technical, analytical, and operational capabilities in support of all of these efforts.

DETECTION TECHNOLOGIES AND SYSTEMS

Every layer of defense requires nuclear detection systems. Radiation detection portals for vehicles and personnel have long been in use at the nation's nuclear weapons complex. Similar instruments, together with access control and material accounting systems, have been installed at numerous sites in Russia and elsewhere to enhance the protection and control of Soviet-legacy weapons-usable nuclear material. Radiation detection instruments are also deployed at foreign border crossings and ports as well as at various entry points into this country. For example, U.S. Customs and Coast Guard inspectors are currently equipped with radiation pagers and low-resolution handheld isotope identifiers. The ORTEC Detective, based on LLNL's high-resolution handheld RadScout isotope identifier, is being deployed and will greatly improve the rapidity and effectiveness of secondary screenings.

Other detection systems have been developed and deployed for road-based and waterway monitoring. For example, LLNL's Adaptable Radiation Area Monitor (which won a 2005 R&D 100 award and is being commercialized) has been demonstrated in challenging urban deployments, including DHS's Countermeasures Testbed. Other deployments at various military bases, under the DTRA's Unconventional Nuclear Warfare Defense program, have demonstrated the ability of innovative algorithms and software packages to integrate the detection signals from a network of sensors to provide tracking and interdiction capabilities. In addition to demonstrating the capabilities of the detection technologies, such real-world deployments are also providing invaluable experience in developing concepts of operations (conops) and coordinating response functions among the various involved agencies.

Other research is under way to develop imaging detectors and new detector materials and to demonstrate next-generation detection concepts. Our overall aim is to develop a suite of detection technologies that (1) are inexpensive to manufacture, operate, and maintain, (2) are able to operate unattended for long periods of time in inhospitable environments, and (3) incorporate data processing, networking, and communications capabilities to provide network-wide, context-aware information. Such systems, when integrated with effective conops, should make it feasible to effectively monitor for nuclear threats (and discriminate non-threat detections) without impeding legitimate commerce or travel.

NUCLEAR SMUGGLING: A KEY NUCLEAR THREAT OBSERVABLE

For more than 25 years, Livermore analysts have assessed incidents of illicit trafficking of alleged nuclear and radiological materials. LLNL maintains comprehensive databases of illicit trafficking incidents, assessments, and related information, providing important insights into this key observable of the larger nuclear terrorism and nuclear proliferation landscape.

With regard to nuclear smuggling trends, and as described in unclassified reports, I am unaware of any illicit trafficking incident pre-dating the dissolution of the Soviet Union that involved potentially weapons-usable nuclear material (e.g., plutonium or highly enriched uranium).

Since 1993, open-source information indicates that there have been roughly a dozen incidents involving significant amounts (gram quantities or larger) of potentially weapons-usable nuclear material. Most of these incidents involved an individual or small group of people, with legitimate access to the material, who opportunistically stole it and subsequently tried to find a buyer. Through their own error and/or law enforcement investigation of the theft, the individuals were apprehended and the material recovered.

LLNL and others have also catalogued hundreds of illicit trafficking incidents in which non-weapons-usable materials, such as radioactive sources, or completely bogus materials, such as lead or mercury, were being trafficked by sellers who claimed to have possession of nuclear material. The traffickers generally asserted that the material was weapons-usable; in some cases, the traffickers claimed that the material was a functional nuclear explosive or “suitcase nuke.”

In light of recent world events, even though nuclear smuggling currently appears to be dominated by scams and driven by opportunists, there is no room for complacency. Each smuggling incident must be carefully assessed on its own merits, as any incident (or collection of incidents) might be the “needle in the haystack” that indicates that a genuine adversary is attempting to or has successfully acquired fissile material or even a weapon diverted from a country’s nuclear stockpile. Attention also needs to be paid to the “big picture,” via assessments of nuclear smuggling incidents in total and linkages to tactical threat incident analysis and strategic and operational analyses, in order to improve interdiction and the identification of threat trends.

THE NEED FOR AN OVERARCHING GLOBAL ARCHITECTURE

Given the multiple U.S. agencies that are responsible for the programs that comprise a defense in depth and the geographic span of the activities, the nation’s efforts to counter nuclear terrorism must be formulated and implemented within an overarching, integrated, global architecture. Given the size and complexity of the endeavor, this architecture must be based on a systematic assessment of risks vs. investments.

This architecture needs to coordinate three critical thrusts—securing nuclear weapons and nuclear materials at their source (domestic and foreign), detecting and tracking the movement (licit and illicit) of nuclear materials, and enhancing U.S. detection, interdiction, and response capabilities.

With a systems approach, we can develop a national investment strategy that allocates resources—technologies, people, effort—where they are most effective. A qualitative and quantitative risk-based framework will allow us to credibly answer such questions as: Which instruments and systems should be deployed and where? Should we deploy more equipment or more people? What new technologies or capabilities are needed to fill which current or anticipated gaps? How can we most effectively work with foreign entities to detect and interdict threats as far from U.S. shores as possible?

Even more important, a global architecture for countering nuclear terrorism will facilitate the critical coordination and sharing of information among the various involved agencies. The

eventual goal with such a system is to be able to fuse detection data and intelligence assessments in a near-real-time environment to achieve overall situational awareness. Such an integrated approach to detection and information analysis will provide dramatic improvement in alarm resolution, threat assessment, trend analysis, and ultimately national defense against nuclear threats.

THE REAL KEY TO DEFENDING AGAINST NUCLEAR TERRORISM

As I've outlined, most of the necessary elements of a "defense in depth" against nuclear terrorism are defined and many are already in place. Work is under way to develop, demonstrate, and deploy increasingly capable nuclear detection systems. Long-standing threat assessment capabilities exist and are being enhanced with novel information extraction and data fusion tools.

But the real key to countering nuclear terrorism is effective coordination among all of the agencies with responsibilities for this exceedingly difficult problem. The 9/11 Commission and WMD Commission reports spelled out very clearly the damage we do to national security when stovepiping and turf battles are the interagency norm. A recent GAO report (June 2005) highlighted the common problem of lack of effective planning and coordination among agencies responsible for combating nuclear smuggling.

Partnership, collaboration, peer review, and communication are needed in order for the nation to successfully defend against nuclear terrorism. Definition of an overall global nuclear defense architecture requires coordination among technologists, policy-makers, and front-line responders, educating each other on what is operationally required, what is technically feasible, and what is politically acceptable. Likewise, technologists, industry, and end-users must collaborate to define technical system requirements, to demonstrate and validate new systems, and to commercialize new technologies and transition new systems into the hands of the end-users. Interagency coordination is equally important in the sharing of threat information and assessments, in implementing and operating the overall defense system, and in responding to and handling real threat incidents.

Cooperation and partnership are needed internationally as well, since much of the "heavy lifting" in countering nuclear terrorism is done abroad—nuclear material protection and control efforts, enhanced border and maritime security, international safeguards and export control regimes, law-enforcement collaboration in investigating trafficking incidents or interdicting suspect shipments, and so forth.

In addition, in light of the difficulty of securing funding for long-term research efforts, it is critical that the various agencies with R&D charters coordinate their efforts, both to make sure the entire spectrum of needed research is covered and to see to it that scientific advances and technology developments supported by one agency are effectively moved from laboratory to deployment. Many of the LLNL technologies that are being deployed to counter nuclear terrorism are the product of many years of support by DOE/NNSA. Working in partnership, DHS, DOE/NNSA, DOD, and other federal agencies can ensure that, in total, the most important problems are being addressed, technology developments are effectively transferred to user

organizations, and the nation's resources (technical talent, facilities, funding, etc.) are optimally applied to counter nuclear terrorism.

CLOSING REMARKS

Unlike the days of the Livermore Study Group, when we talked of the need to prepare for the “catastrophic maybe” of WMD terrorism, there is widespread recognition of the reality, severity, and enduring nature of the terrorist threat, particularly the threat of nuclear terrorism. This recognition is being translated into increased funding for the organizations and programs chartered to counter terrorism and secure the U.S. homeland. Included in this increased funding are critical monies for the long-term R&D needed to generate the technological breakthroughs that will be required to turn counterterrorism concepts into effective operational systems. However, even as the nation increases its focus on protecting the homeland against nuclear terrorism, it is essential to continue support for the programs that provide early-stage defense in securing and interdicting nuclear material, the information analysis and data mining efforts to search for and provide early warning of specific threat activities, and the emergency response capabilities that enable the nation to deal effectively with the full range of nuclear terrorist threats.

Just as U.S. scientific and technological superiority helped secure the peace during the Cold War, science and technology are key to winning the war against terrorism. However, terrorists are innovative, resourceful, and committed. Thus, we must be even more innovative, resourceful, and committed to thwarting their attempts to harm to this country and its citizens. WMD terrorism is an enduring threat, and the nation must prepare for the long haul. In particular, programs in proliferation prevention, counterterrorism, and homeland security require sustained investment. They are closely linked and must not be selected “either/or”; neither can they be conducted in isolation from one another. It is critical that we work to ensure effective coordination, collaboration, and communication among the many departments and agencies with responsibilities for proliferation prevention, counterterrorism, and homeland security.

We at LLNL have long been concerned about the terrorist nuclear threat. We have built on our historical nuclear weapons mission and developed expertise, capabilities, and technologies to meet this threat. LLNL is already providing critical elements of the nation's defense against nuclear, chemical, and biological terrorism. Our hallmark approach of integration—across technical disciplines and among R&D institutions, sponsors, and end-users—is well suited to the nuclear terrorism challenge. We are committed to using our scientific and technological resources to meet the nation's national security needs today and in the future.